ChangeGroup

NIS2 – EU's nye It-sikkerhedsdirektiv

Karsten Dahl Vandrup

It-sikkerhedsspecialist - Lektor

sammen om digital transformation

AGENDA

Hvorfor et Cybersikkerheds Direktiv

Hvad er NIS2?

Hvilke krav stiller NIS2 til virksomhederne?

Beredskabsplan

Hvem bliver omfattet af det nye NIS2-direktiv?

Hvornår træder NIS2 i kraft?

Hvad anbefaler CHANGE GROUP?

ChangeGroup

Hvorfor et nyt Cyber Security Direktiv netop nu?

- Cyber crime er i hastig vækst
- Vi er dårligt forberedt
- Danmark er som en gennem-digitaliseret nation særligt udsat
- Nye metoder til kriminalitet ser dagens lys dagligt
- Krigen i Ukraine har fået Cybertruslen op på det maksimale

ChangeGroup

Hvad er NIS2

NIS2s tre hovedmål er:

- at øge IT-modstandsdygtigheden på tværs af væsentlige tjenesteudbydere
- at strømline modstandsdygtigheden gennem strengere sikkerhedskrav og sanktioner for overtrædelser
- at forbedre EU's beredskab til at håndtere IT-angreb.

Minimumskrav til sikkerheden

Direktivet opdeler virksomheder i ‘essentielle’ og ‘vigtige’, hvor der er en forskel i bødeniveau for at overtræde kravene om sikkerhedsforanstaltninger og anmeldelsespligten.

Essentielle virksomheder risikerer en bøde på op til 10 millioner euro eller 2 procent af den globale årlige omsætning, hvor vigtige virksomheder risikerer bøder på op til 7 millioner euro eller 1,4 procent af den globale årlige omsætning.

ChangeGroup

Hvilke krav stiller NIS2 til virksomhederne?

ChangeGroup

Hvad kræver NIS2 som minimum

Virksomheden skal tage højde for 'state of the art'-teknologi, samt europæiske og internationale standarder. Direktivet indeholder dog en række minimums-tiltag, som man skal implementere.

Foranstaltningerne skal som minimum indeholde:

- Risikovurderinger og sikkerhedspolitikker for informationssystemer (ISO)
- En plan for at håndtere sikkerhedshændelser (ISO)
- En plan for forretningens drift under og efter en sikkerhedshændelse, og det betyder, at ens backups skal være opdateret. Man skal også have en plan for at sikre adgang til it-systemer og deres funktioners drift under og efter en sikkerhedshændelse. (ISO)

(ISO = Ca. Samme krav som i ISO 27001

ChangeGroup

Hvad kræver NIS2 som minimum

- Sikkerhed omkring forsyningskæder og forholdet mellem virksomheden og direkte leverandører. Virksomheder skal vælge sikkerhedsforanstaltninger, der passer til sårbarheder hos den enkelte direkte leverandør. Og så skal virksomheder vurdere det overordnede sikkerhedsniveau for alle leverandører. (ISO)
- Sikkerhed omkring indkøb af systemer og udviklingen og drift af systemer. Det betyder også, at man skal have politikker for, hvordan man håndterer og indrapporterer sårbarheder. (ISO)
- Politikker og procedurer for at vurdere, hvor effektive sikkerhedsforanstaltningerne er. (ISO)
- Cybersikkerhedstræning og en praksis for elementær computer-hygiejne (ISO)

(ISO = Ca. Samme krav som i ISO 27001

ChangeGroup

Hvad kræver NIS2 som minimum

- Politikker og procedurer for brugen af kryptografi og, når det er relevant, kryptering. (Ikke direkte et krav i ISO)
- Sikkerhedsprocedurer for medarbejdere med adgang til følsomme eller vigtige data, herunder politikker for adgang til data. Virksomheden skal også have et overblik over alle relevante aktiver og sørge for, at de bliver udnyttet og håndteret ordentligt. (ISO)
- Brugen af multifaktor-godkendelse, 'continuous authentication'-løsninger, stemme-, video- og tekst-kryptering og krypteret intern nødkommunikation, når det giver mening. (ISO-agtigt – men udvidet/skærpet)

(ISO = Ca. Samme krav som i ISO 27001

ChangeGroup

Incident Response & Business Continuity

ChangeGroup

Indenfor de første 24 timer

Det ikke nok bare at implementere en række sikkerhedsforanstaltninger. Hvis man bliver udsat for en væsentlig sikkerhedshændelse, skal man anmelde det til en relevant myndighed (som ikke er udpenslet mere konkret i direktivet) eller CSIRT (Computer Security Incident Response Team, som medlemslande skal etablere).

I teksten står der, at en sikkerhedshændelse væsentlig, hvis den kan lede til alvorlige driftsforstyrrelser eller økonomiske tab for virksomheden, eller hvis hændelsen kan føre til betydelige tab for andre.

Den første anmeldelse (early warning) til CSIRT* eller den relevante myndighed skal ske senest 24 timer efter, man er blevet bekendt med bruddet. Man skal fortælle, om man mener, at ondsindede aktører er involveret, og om hændelsen kan påvirke andre medlemslande.

*) CSIRT (Computer Security Incident Response Team), i Danmark: CFCS

Indenfor de første 72 timer, og derefter

Senest 72 timer efter, man har opdaget bruddet, skal virksomheden opdatere (incident notification) den første anmeldelse med en umiddelbar vurdering af hændelsen, hvor alvorlig den er, hvor stor indvirkning den vil have og, hvis de er tilgængelige, kompromitteringsindikatorer.

Senest en måned efter 'incident notification' skal virksomheden aflægge en endelig rapport, der som minimum skal indeholde en detaljeret beskrivelse af hændelsen, og hvor alvorlig den er; hvilken type af trussel, der sandsynligvis førte til hændelsen; hvad man har gjort og stadig gør for at forebygge skaden; og hændelsens eventuelle indvirkning uden for Danmark.

Hvis ikke virksomheden er færdig med at håndtere bruddet, når man skal aflægge den endelige rapport, skal man i stedet indsende en statusrapport. Den sidste anmeldelse skal så ske senest én måned efter, hændelsen er afsluttet.

ChangeGroup

Hvem

bliver omfattet af det nye NIS2-direktiv?

ChangeGroup

Hvem bliver omfattet af det nye NIS2-direktiv?

NIS2 kommer til at omfatte en række nye sektorer og private aktører, der ikke har været omfattet af det nuværende NIS-direktiv.

Desuden går NIS2 væk fra den hidtidige sondring mellem vigtige tjenester og digitale tjenester og fokuserer i stedet på væsentlige og vigtige enheder inden for en række sektorer baseret på:

- Den sektor, organisationerne opererer i, og de leverede tjenester
- Vigtigheden af sektoren og de leverede tjenester
- Afhængighedsforhold til andre sektorer

ChangeGroup

Hvem bliver omfattet af det nye NIS2-direktiv?

Det oprindelige NIS-direktiv omfatter organisationer i følgende sektorer:

Sundhed

Digital infrastruktur

Transport

Vandforsyning

Digitale tjenesteudbydere

Bank- og finansmarkedsinfrastruktur

Energi

Det nye NIS2-direktiv tilføjer:

Udbydere af offentlige elektroniske kommunikationsnetværk eller -tjenester

Spildevand og affaldshåndtering

Fremstilling af ekstra vigtige produkter (f.eks. lægemidler, medicinsk udstyr og kemikalier)

Fødevarer

Digitale tjenester (f.eks. sociale netværksplatforme og datacentertjenester)

Rummet (f.eks. rumfart)

Post- og kurertjenester

Offentlig administration

ChangeGroup

Essentielle og vigtige virksomheder

Direktivet gælder for virksomheder i en række sektorer listet i NIS2, herunder energi, fødevareproduktion og rumfart. Hvis det er store virksomheder, er de 'essentielle', og hvis de er mellemstore virksomheder, er de 'vigtige'.

Derudover er 'essentielle' virksomheder:

- Kvalificerede “trust service providers” og “top-level domain name registries” og “DNS service providers” uanset størrelse.
- “Public electronic communications networks” eller “publicly available electronic communications services”, som er store virksomheder.
- Et medlemslands centraladministration og regioner.
- Andre virksomheder, der tilhører sektorer på listen, som Danmark har vurderet er kritiske i forhold til at opretholde den nationale sikkerhed.

Essentielle og vigtige virksomheder

Loven kræver, at både essentielle og vigtige virksomheder implementerer tekniske, driftsmæssige og organisatoriske foranstaltninger for at kunne håndtere de risici, som truer deres systemer. Det gælder både systemer, der bidrager til forretningens drift og den tjeneste, man leverer, men også for at skåne andre virksomheder eller kunder mod angreb.

Når en virksomhed skal vurdere, hvilke foranstaltninger man skal implementere, skal man tage højde for, hvor udsat virksomheden er overfor trusler og ens størrelse. Man skal også tage med i overvejelsen, hvor sandsynligt det er, at forretningen udsættes for sikkerhedshændelser, og hvor alvorlige de er – især i forhold til deres samfundsmæssige og økonomiske indvirkning.

Hvornår træder NIS2 i kraft

20 dage efter NIS2 offentliggøres på EU's officielle portal for lovtekster (sandsynligvis til september 2022, oplyser Europa-Parlamentet), har medlemslandene 21 måneder til at lave nationale bekendtgørelser.

Når de er færdige, kommer direktivets regler til at gælde i Danmark.

ChangeGroup

Ledelsen kan stilles til ansvar

Lovteksten understreger, at en virksomheds ledelse kan blive stillet til ansvar for brud med sikkerheds- og anmeldelsespligten og skal gennemgå kurser for at blive bedre til at vurdere cybersikkerhedsrisici.

Samtidig skal ledelsen opfordre virksomheden til at tilbyde lignende kurser til alle medarbejdere regelmæssigt.

Derfor er flere eksperter enige om, at danske organisationer allerede nu bør forberede sig på kravene, selvom de nok først kommer til at gælde i Danmark om to år.

Hvad anbefaler Change Group?

- At I får et overblik over hvad der kræves af jeres virksomhed/organisation
- At I laver en GAB-analyse: Hvor er vi, og hvor skal vi hen?
- At I laver en implementeringsplan
- At I overvejer hvilke kompetencer og ressourcer der skal til
- At I finder ud af hvilken hjælpe I skal have udefra

CHANGE GROUP HAR EKSPERTERNE, OG HJÆLPER GERNE MED DETTE!

ChangeGroup

ChangeGroup

Karsten Dahl Vandrup
It-sikkerhedsekspert
Mobil: +45 5076 2764
Email: kava@stealthcomputing.dk

Lyngbyvej 2
DK-2100 København Ø
Telefon: 3332 7778

www.changegroup.dk

sammen om digital transformation